7. OTHER OBLIGATIONS

In addition to the obligations presented so far, the GDPR imposes other obligations to the Controller.

The first of these **obligations are data protection policies**, for which the GDPR does not specify what their content should be. These policies are configured as one of the technical and organizational measures to be taken by the controller, which should include information on the data processing carried out by the organization, as well as its commitments in relation to data protection (for example, identification of the Controller and Data Protection Officer, how rights can be exercised, etc.).

The next obligation is the **record of processing activities** (RAT). The RAT has replaced the previous obligation to register files with Control Authorities, a procedure that disappeared with the GDPR. Public sector entities, such as City Councils, are obliged to have this Register.

The GDPR establishes the content of the Register (purposes of the processing, categories of data subjects and personal data, and a general description of the technical and organizational security measures, among others).

In certain cases, the obligation to have the RAT, with similar content, is also applicable to Data Processors, and the Data Controller on behalf of whom the Data Processor works, must be also identified.

The following is an explanation of Data Protection by Design and Data Protection by Default. First of all, **Data Protection by Design** involves taking into account all the obligations and requirements imposed by data protection regulations, from the moment a new treatment is designed. In particular, it requires the implementation of appropriate technical and organizational measures, such as pseudonymization; effectively apply data protection principles; and integrate the necessary guarantees to comply with the obligations imposed by the GDPR and to protect the rights of the concerned data subjects. For example, if a local entity decides to create an electronic channel that allows citizen participation, before implementing it, it must evaluate whether it is necessary to identify data subjects, what data is collected, how to ensure data security, how they can exercise their rights, etc.

And secondly, **Data Protection by Default** is the principle according to which an organisation (the data controller) ensures that only the data strictly necessary for each specific purpose of the processing are processed by default (without the intervention of the user). Thus, when a person registers on a social network, data protection by default would mean that, without having to configure anything, the profile should be private. And the other way around, if the user wants it to be public, this modification must be made by him.

The European Regulation also **requires that appropriate or adequate measures be taken to ensure data security**. Proper risk analysis should be performed to determine appropriate security measures.

The risk analysis should take into account the following elements: the nature of the data (e.g. whether special categories of data are processed), the number of concerned data subjects or the amount (volume of data), or the variety of processing (e.g. whether it allows profiling).

The GDPR states that security measures may consist of:

- Minimize data processing.
- The pseudonymization or encryption of data.
- The ability to ensure the confidentiality, integrity, availability and continuous resilience of processing systems and services, i.e. the ability to resist or recover (e.g. from a hacker attack).

- The ability to restore availability and access to personal data quickly, in the event of a physical or technical incident (e.g. with backups).

- A process for regularly verifying, evaluating, and evaluating the effectiveness of security measures. For example, this would be achieved through audits of these measures.

Another obligation is **to report security breaches**. This obligation implies that, in the event of any breach or incident of data security that is suffered and means a risk to the rights and freedoms of the concerned data subjects, the City Council responsible for the treatment must notify it to the competent Control Authority. This notification must be made without delay, no later than 72 hours after the time of the violation. However, if the violation is unlikely to constitute a risk to the rights and freedoms of individuals, such notification is not necessary.

In cases where the Control Authority has to be notified since the risk cannot be considered unlikely, if the Local Authority considers that the breach of security may pose a high risk to the rights and freedoms of individuals, in addition to notifying the Control Authority, **the concerned data subjects should be notified**, and should be offered recommendations to mitigate risks.

In any case, in the event of any type of incident that may affect the security of the data, even in cases that do not require notification to the Authority, the responsible local body must **document the incident internally**, noting the facts and the corrective measures adopted. This internal documentation shall be made available to the Control Authority so that it can carry out the corresponding checks.

Finally, the appointment of **a Data Protection Officer** (DPO) is mandatory in certain cases, and in any case when the Data Controller or Data Processor is an Authority or Public Body. Therefore, a City Council is required to have a DPO. However, the same DPO can be designated for several entities.

The DPO is the organization's benchmark in data protection, which, among other requirements, must have experience in this area.

The functions of the DPO are described in the data protection regulations. The most relevant are:

- It must inform and advise the Data Controller or the Data Processor, as well as its employees, on the obligations they must comply with in terms of data protection.

- It is also responsible for monitoring compliance with data protection regulations and the policies of the Data Controller or the Data Processor r, including the allocation of responsibilities, staff awareness and training, and related audits.